# Strategic Economic Decision-Making:
# Using Bayesian Belief Networks to Make Complex Decisions

A Presentation Highlighting the Capabilities of the BayeSniffer Algorithm

Dr. Jeff Grover, Sr., The DataSniffer
DBA Consulting, Inc., Chief Data Scientist
https://BayeSniffer.com

Reviewed by Mr. Jeff Grover, Jr., PhD. Student
University of Kentucky, Department of Economics

Presented to MORS
Washington, DC
10/14/14

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| | | |
|---|---|---|
| 1. REPORT DATE<br>**14 OCT 2014** | 2. REPORT TYPE | 3. DATES COVERED<br>**00-00-2014 to 00-00-2014** |

| | |
|---|---|
| 4. TITLE AND SUBTITLE<br>**Strategic Economic Decision-Making: Using Bayesian Belief Networks to Make Complex Decisions** | 5a. CONTRACT NUMBER<br>5b. GRANT NUMBER<br>5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER<br>5e. TASK NUMBER<br>5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**DBA Consulting, Inc,512 Maplecrest Way,Elizabethtown,KY,42701** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S)<br>11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES
**presented at the How Risk Assessments Inform National Security Decision Making, 14-17 October 2014 held in Alexandria, VA. Sponsored by the Military Operations Research Society (MORS) and the Security Analysis and Risk Management Association (SARMA).**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT<br>**unclassified** | b. ABSTRACT<br>**unclassified** | c. THIS PAGE<br>**unclassified** | **Same as Report (SAR)** | **28** | |

**Standard Form 298 (Rev. 8-98)**
Prescribed by ANSI Std Z39-18

The DataSniffer

# Executive Summary

- By nature, **big data** stored or warehoused in organizational storage facilities does not immediately suggest courses of action to maximize revenues, minimize costs or does it suggest optimal results.
- The challenge of any organization is to extract actionable **business intelligence** solutions from these data.
- We suggests the use of a **server-based algorithm** as a unique **discrete** data-sniffing tool to translate **structured data** into business intelligence through a **Structured Query Language** (SQL) server-based approach.
- The concept of a **server-based algorithm** follows empirical research on Bayesian belief networks (BBN) and the publication of *Strategic Economic Decision-Making: Using Bayesian Belief Networks to Solve Complex Problems* (Grover, 2013).

# Executive Summary (Continued)

- We interpret the results of a **server-based algorithm inductively** to provide a consistent translation of the analysis we obtain from the use of BBN.
- With the deluge of **data-mining protocols** available in the market today, a niche should be in evaluating structured data information and translating it into business intelligence using **conditional probabilities** derived from the **axioms of set theory and Bayes' theorem**.
- This presentation gives an overview of the problems organizations face, suggests the use of an **server-based algorithm** as a solution, reviews Bayes' theorem as it applies to the algorithm, and gives a real-world example of data sniffing statistical capabilities.

# Executive Summary (Continued)

- Analyzing big data is a **massive undertaking** for large and complex organizations.
- Large organizations must pull data from **many different sources**, such as research experiments, consumer choice selections, production chains, crop yields, government databases, et cetera.
- The process of **compiling**, **uploading**, and **parsing** through these data is very **labor-intensive** and **monetarily expensive**.
- Furthermore, properly extracting the information contained in these data and translating it into business strategies is a **Herculean task**.
  - Different results from the same datasets due to **different interpretations**.
  - **Human error** at any step in the process
- Obstacles must be overcome when converting **data information** to **business intelligence**.
- The challenge is **capturing all available intelligence.**

# Executive Summary (Continued)

- Some may think **generic data mining** is the solution, but we must take care to ensure that organizations are doing more than just ”fishing” through the data, or calculating meaningless correlations, which seems to be the hallmark of big name data mining services.
- Remember, a higher expected standard is to **replicate** data results
  - ”**Fishing expeditions**” do not allow for this expectation to be met.
- **Exploiting** data we encourage decision makers to ensure their data is being fully exploited
  - A must in executive-level decision-making. 100mb data = One Million Dollars (Rankins, R, Bertucci, P, Gallelli, C, & Silverstein, A (2013)).
- Is there a way to **seamlessly collate** this information?

# Executive Summary (Solution)

- **Overcoming obstacles**
  - **Traditional (frequentist) statistical methods vs Non traditional (subjective view)**
    - **Big Data** suggest populations are being maximized so estimates of the population no longer To overcome the issues that traditional statistical techniques create, we propose the use of the **BayeSniffer**, a **proprietary SQL server-based algorithm** that ``**sniffs**'' through big data and extracts business intelligence using Bayes' theorem of conditional probabilities rather than estimating traditional (frequentist) relationships or those big data correlations.
- The **server-based algorithm** analyzes tables that contain information about possibly independent events, and deduces the conditional probabilities between those events. The algorithm evaluates the **priors** in the data, uses them with **likelihoods** to calculate **joints**, and finally produces useful results in the form of **posterior** probabilities.
- We turn to a discussion of **Bayes' theorem** and its application of **BBN** in a **server-based algorithm**.

# Bayes' Theorem: An Introduction

- Bayes' theorem and its application in **Effective SEDM**

$$P(B_i|A) = \frac{P(AB_i)}{P(A)}$$

- This is the classic equation for Bayes' theorem in its simplest form.
  - It reads the **conditional probability** of event Bi occurring given event A is equal to the joint probability of events A and Bi, divided by the marginal probability of event A."
  - Here, Bi is the ith event out of k mutually exclusive (ME) and collectively exhaustive (CE) events.
- We expand this equation using the **chain rule of probability**, which states that the joint probability of events A and Bi is equal to the conditional probability of event A given the probability of event Bi, times the probability of event Bi:

$$P(AB_i) = P(A|B_i)P(B_i)$$

# Bayes' Theorem Proof

- Substituting the chain rule into Bayes' theorem yields:

$$P(B_i|A) = \frac{P(A|B_i)P(B_i)}{P(A)}$$

- Which brings us to a simple proof of Bayes' theorem (relaxing Bi):

$$P(BA) = P(AB)$$

$$P(BA) = P(B|A)P(A)$$

$$P(AB) = P(A|B)P(B)$$

$$P(B|A)P(A) = P(A|B)P(B)$$

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)} = \frac{P(AB)}{P(A)} = \frac{P(BA)}{P(A)}$$

# Bayes' Theorem Proof (Con't)

- Here, there are two events: the **unknown prior event**, event B, and the observable information event, event A.
- Let us view each of these events as **discrete column vectors** consisting of two or more ME elements. In a BBN, this configuration can be illustrated in the Figure below where this **sample space** consist of two CE events (B and A) where each has two ME elements: B1, B2 and A1, A2, respectively.


This Figure represents a two-node, two-event BBN. We can break down this network into four subcategories based on whether or not the elements of event A correct classify the elements of event B. This is represented by the following **truth table**.

# Bayes’ Theorem Proof (Con’t)

| EVENT A | EVENT B | |
|---|---|---|
| | Positive (B1) | Negative (B2) |
| Positive (A1) | True Positive<br>= B1%<br>= P(B1\|A1) | False Positive<br>= 100% - B2%<br>= P(B1\|A2) |
| Negative (A2) | False Negative<br>= 100% - B1%<br>= P(B2\|A1) | True Negative<br>= B2%<br>= P(B2\|A2) |

- This BBN **truth table** shows the relationship between the accuracy of the observable information contained in event A and the prior (**unobservable**) information contained in event B. In this two-node, two-event BBN, the classical outcomes are:
  - **True Positive**: the elements in event A1 correctly classify those in event B1: P(B1|A1)
  - **False Positive**: the elements in event A1 incorrectly classify those in event B2: P(B2|A1)
  - **False Negative**: the elements in event A2 incorrectly classify those in event B1: P(B1|A2)
  - **True Negative**: the elements in event A2 correctly classify those in event B2: P(B2|A1)

# Decision Tree

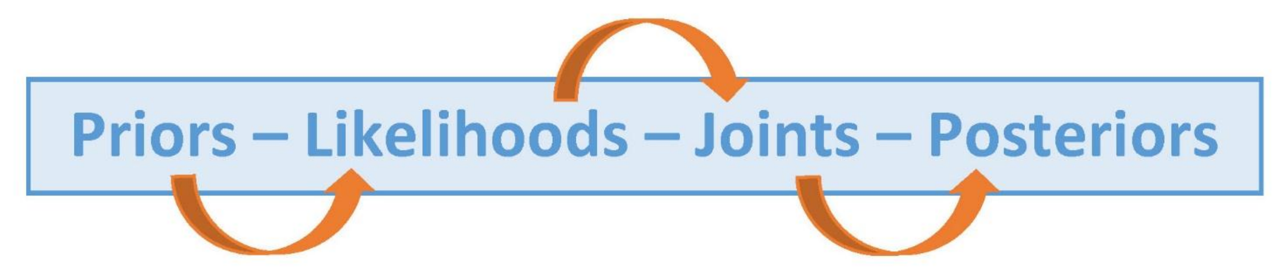
**PROBABILITIES**

| Priors | Marginals | Likelihood | Joints | Marginals | Posteriors |
|---|---|---|---|---|---|
| | P(A1) + | $P(A1 \mid B1)$ | P(B1,A1) | True + | $P(B1 \mid A1)$ |
| P(B1) + | | | | P(A1) | |
| | P(A2) - | $P(A2 \mid B2)$ | P(B1,A2) | False - | $P(B1 \mid A2)$ |
| | P(A1) + | $P(A1 \mid B1)$ | $P(B2 \mid A1)$ | False + | $P(B1 \mid A1)$ |
| P(B2) - | | | | P(A2) | |
| | P(A2) - | $P(A2 \mid B2)$ | $P(B2 \mid A2)$ | True - | $P(B1 \mid A2)$ |

- The decision tree starts with the priors, P(Bi), the **unconditional probabilities** that are unobserved. (Note, we can now gather them from big data and use as a **proxy** for the population.)
  - It turns out that this is acceptable due to the learning that occurs by the algorithm when we add multiple observable events to the BBN.
- From here, we compute the **likelihoods** (through the **marginal** of Ai), P(A1|B1),
- The **joints**, (P(A1,B1),
- And finally the **posteriors** (through the **marginal** of Ai), P(B1|A1).

# Bayes' Process

- These **posteriors** are the true probabilities that we seek; they express information hidden within the priors that is not immediately discernable from the data.
- The **posterior**, for example P(B1|A1), is the probability of event B1 will occur given that event A1 had already occurred.
- Using Bayesian statistics, we can compute any combination of **posteriors**. Most importantly, we can generalize BBN to represent n-event models.



# Bayes' theorem

- Now, this is all we need to know to sniff business intelligence from data information:

$$P(B_i|A) = \frac{P(AB_i)}{P(A)}$$

- Think of Bayes' theorem as plutonium for a nuclear bomb and the chain rule as a joint probability generating machine.

*Now we are armed with a simple tool to slice thorough a sequence of CE events that contain discrete ME elements in any sample space.*

# Real World Scenario

- I will use the **BayeSniffer** server-side algorithm to demonstrate the utility of BBN in answering a series of hypotheses.

- The **Global Terrorism website** maintains a database consisting of historical terrorist incidences.

- In this example, we aim to answer **two questions** (hypotheses):

--1. What type of terrorist attack (AT) is most likely to occur in a given region (R)?

**--P(AT|R)**

--2. Where is a given type of terrorist attack most likely to occur?

**--P(R|AT)**

# Real World Scenario

- The Global Terrorism database contains **113,113 observations** of terrorist attacks that records the region of the world where the attack occurred (13 categories), and the type of attack (9 categories).

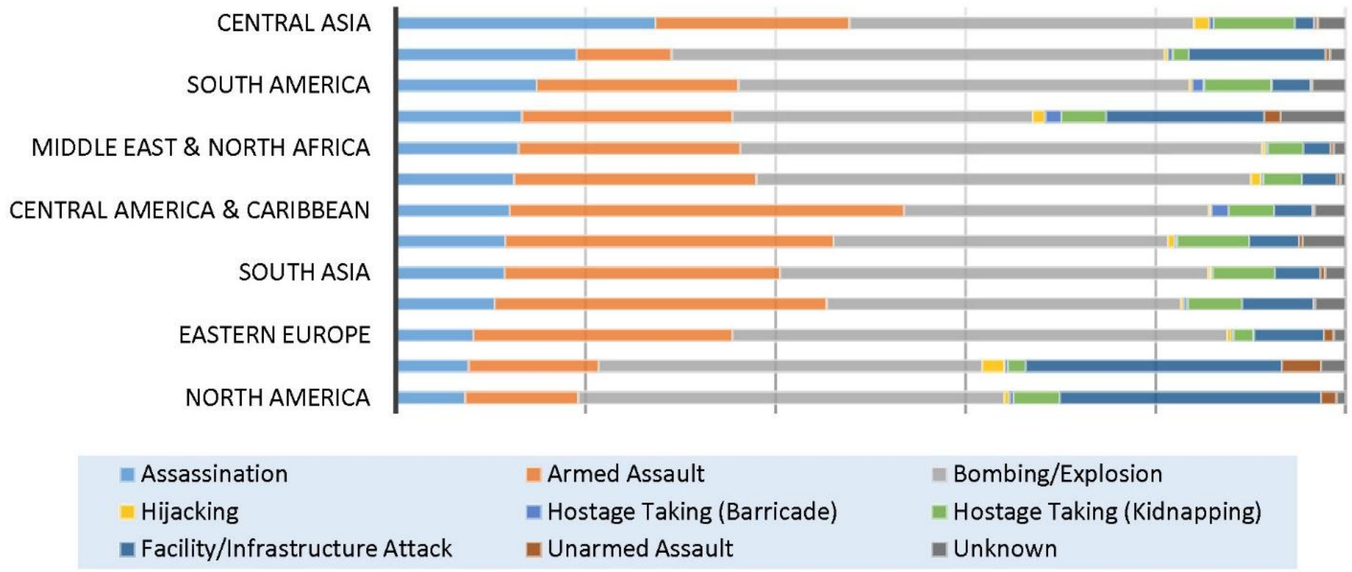
- After sniffing the data, the BayeSniffer answered the first question by calculating the following **posteriors**, $P(ATj|Ri)$. Suppose we are interested in knowing what type of attack is most likely to occur in a given region.

# Posterior Results

| Region P(R) | Attack Type P(AT) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Assassi-nation | Armed Attack | Bomb-ing | Hijack-ing | Hostage Bombing | Hostage Kidnap-ping | Facility | Unarme d Assault | Un-known | TOTAL |
| North America | 7.29% | 11.95% | 44.82% | 0.55% | 0.45% | 4.87% | 27.49% | 1.62% | 0.97% | 100.00% |
| Central America & Caribbean | 11.95% | 41.57% | 32.10% | 0.25% | 1.81% | 4.82% | 4.05% | 0.19% | 3.26% | 100.00% |
| South America | 14.82% | 21.25% | 47.45% | 0.37% | 1.24% | 7.12% | 4.09% | 0.23% | 3.43% | 100.00% |
| East Asia | 7.68% | 13.66% | 40.40% | 2.42% | 0.28% | 1.85% | 27.03% | 4.13% | 2.56% | 100.00% |
| Southeast Asia | 10.39% | 34.99% | 37.28% | 0.36% | 0.38% | 5.71% | 7.52% | 0.16% | 3.22% | 100.00% |
| South Asia | 11.43% | 29.03% | 45.11% | 0.30% | 0.11% | 6.60% | 4.77% | 0.50% | 2.15% | 100.00% |
| Central Asia | 27.35% | 20.41% | 36.33% | 1.63% | 0.41% | 8.57% | 2.04% | 0.41% | 2.86% | 100.00% |
| Western Europe | 19.03% | 9.97% | 51.92% | 0.36% | 0.50% | 1.72% | 14.42% | 0.47% | 1.61% | 100.00% |
| Eastern Europe | 8.18% | 27.29% | 52.12% | 0.39% | 0.20% | 2.17% | 7.39% | 0.99% | 1.28% | 100.00% |
| Middle East & North Africa | 12.89% | 23.38% | 54.99% | 0.37% | 0.18% | 3.74% | 2.89% | 0.32% | 1.25% | 100.00% |
| Sub-Saharan Africa | 11.55% | 34.51% | 35.23% | 0.69% | 0.27% | 7.66% | 5.24% | 0.38% | 4.49% | 100.00% |
| Russia & NIS | 12.47% | 25.46% | 52.11% | 1.07% | 0.26% | 4.06% | 3.67% | 0.38% | 0.51% | 100.00% |
| Australasia & Oceania | 13.25% | 22.22% | 31.62% | 1.28% | 1.71% | 4.70% | 16.67% | 1.71% | 6.84% | 100.00% |

We read these posteriors as: P(ATj|Ri). Or for example, P(AT = Bombing|R = Sub-Saharan Africa) = 35.23%.

We also represent these results as a stacked bar graph in the figure below.



# Posterior Results (Con't)

- From these results, we can observe and rank the likelihoods of different attack types occurring in each region of the world. In **Sub-Saharan Africa**, the most **likely types of attacks are bombings** (35.23%) and armed attacks (34.51%), with the least likely types being hostage bombings (0.27%) and unarmed assaults (0.38%).

- We can also use the algorithm to answer our second question **and the most likely region of the world where a certain attack will take place**, or **P(R|AT).** Suppose we want to know where an **assassination** is most likely to occur.

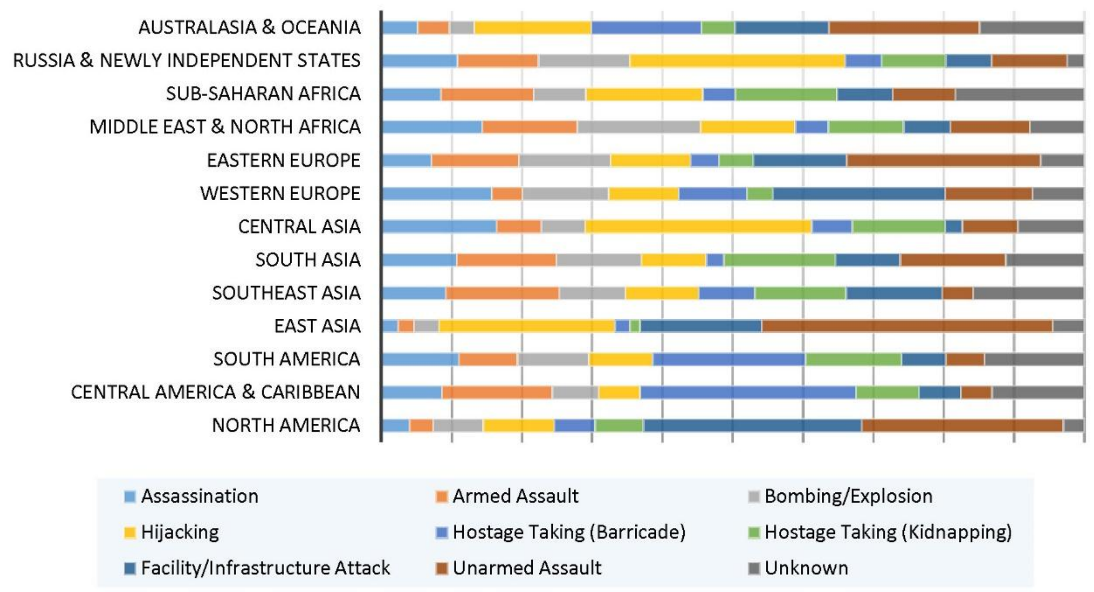
# Posterior Results (Con't)

| Attack Type P(AT) | Region P(R) | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | North America | Central America & Caribbean | South America | East Asia | Southeast Asia | South Asia | Central Asia | Western Europe | Eastern Europe | Middle East & North Africa | Sub-Saharan Africa | Russia & NIS | Australasia & Oceania | TOTAL |
| Assasi-nation | 1.42% | 8.47% | 17.90% | 0.36% | 4.90% | 18.16% | 0.45% | 19.30% | 0.56% | 19.99% | 6.33% | 1.96% | 0.21% | 100.00% |
| Armed Attack | 1.21% | 15.31% | 13.33% | 0.33% | 8.56% | 23.95% | 0.17% | 5.25% | 0.97% | 18.83% | 9.83% | 2.08% | 0.18% | 100.00% |
| Bombing | 2.49% | 6.50% | 16.37% | 0.54% | 5.02% | 20.48% | 0.17% | 15.04% | 1.01% | 24.37% | 5.52% | 2.34% | 0.14% | 100.00% |
| Hijacking | 3.54% | 5.75% | 14.60% | 3.76% | 5.53% | 15.49% | 0.88% | 12.17% | 0.88% | 18.81% | 12.39% | 5.53% | 0.66% | 100.00% |
| Hostage Bombing | 2.04% | 30.03% | 35.06% | 0.31% | 4.25% | 4.25% | 0.16% | 11.95% | 0.31% | 6.60% | 3.46% | 0.94% | 0.63% | 100.00% |
| Hostage Kidnap. | 2.43% | 8.76% | 22.06% | 0.22% | 6.90% | 26.93% | 0.36% | 4.48% | 0.38% | 14.88% | 10.78% | 1.64% | 0.19% | 100.00% |
| Facility | 10.92% | 5.87% | 10.10% | 2.61% | 7.25% | 15.51% | 0.07% | 29.90% | 1.03% | 9.15% | 5.87% | 1.18% | 0.54% | 100.00% |
| Unarmed Attack | 10.09% | 4.29% | 8.80% | 6.22% | 2.36% | 25.32% | 0.21% | 15.24% | 2.15% | 15.88% | 6.65% | 1.93% | 0.86% | 100.00% |
| Unknown | 1.04% | 12.83% | 22.95% | 0.67% | 8.41% | 18.90% | 0.26% | 9.04% | 0.48% | 10.71% | 13.65% | 0.45% | 0.60% | 100.00% |

We read these posteriors as: P(Ri|ATj). Or for example, P(R = Sub-Saharan Africa|AT = Bombing) = 5.52%.

*Note: P(Ri|ATj) ≠ P(ATj|R)*

- Here we see that an **assassination** is *most likely* to occur in the **Middle East & North Africa** (19.99%) or **Western Europe** (19.30%), and *least likely* to occur in **Australasia & Oceania** (0.21%) and **East Asia** (0.36%).



# Why Use Bayes' Theorem?

- If deductive hypothesis testing is the standard for statistical analysis, then why use **inductive reasoning**? In the above example, there are thirteen regions (Event A) and nine attack types (Event B). This makes a total of **117 different paths (hypotheses)** the decision tree branches and that's just a **two-event** BBN.

- When generalized to n events, the number of paths increases. For example, we could extend the terrorism example to include the **22 target types** recorded by the database, resulting in **13 x 9 x 22 = 2,574** paths to evaluate.

# Why Use Bayes' Theorem & BBN?

- A more realistic real world BBN can have **13 x 9 x 22 x 15 x 10 = 386,100 paths** to evaluate. A human simply does not have the capability to logically low through these paths manually and make a decision; but a server-based BBN algorithm similar to the BayeSniffer has that ability.

- Taking most of the information in the 113,113 rows of information contained in the Global Terrorism database, there are this many hypotheses to select from:

| | | |
|---|---|---|
| gname | 3182 | 70,361,047,920,354,400,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 |

- So the question becomes, which path will the terrorist take next?

***"Big Problem = Server Based BBN Algorithm"***

# # Paths (Rows)

| Event | # ME-E | # Paths (Rows) |
|---|---|---|
| extended | 2 | 2 |
| crit1 | 2 | 4 |
| crit2 | 2 | 8 |
| crit3 | 2 | 16 |
| gsubname3 | 2 | 32 |
| guncertain1 | 2 | 64 |
| vicinity | 3 | 192 |
| doubtterr | 3 | 576 |
| multiple | 3 | 1,728 |
| success | 3 | 5,184 |
| suicide | 3 | 15,552 |
| guncertain2 | 3 | 46,656 |
| guncertain3 | 3 | 139,968 |
| INT_LOG | 3 | 419,904 |
| INT_IDEO | 3 | 1,259,712 |
| INT_MISC | 3 | 3,779,136 |
| INT_ANY | 3 | 11,337,408 |
| alternative | 4 | 45,349,632 |
| alternative_txt | 4 | 181,398,528 |
| claim3 | 4 | 725,594,112 |
| compclaim | 4 | 2,902,376,448 |
| ishostkid | 4 | 11,609,505,792 |
| ransom | 4 | 46,438,023,168 |
| claimed | 5 | 232,190,115,840 |
| specificity | 6 | 1,393,140,695,040 |
| property | 6 | 8,358,844,170,240 |
| propextent | 6 | 50,153,065,021,440 |
| weaptype4_txt | 8 | 401,224,520,171,520 |

| Event | # ME-E | # Paths (Rows) |
|---|---|---|
| attacktype3_txt | 9 | 3,611,020,681,543,680 |
| claimmode3_txt | 10 | 36,110,206,815,436,800 |
| weaptype3_txt | 11 | 397,212,274,969,805,000 |
| claimmode2_txt | 12 | 4,766,547,299,637,660,000 |
| weaptype2_txt | 12 | 57,198,567,595,651,900,000 |
| propextent_txt | 12 | 686,382,811,147,823,000,000 |
| attacktype2_txt | 13 | 8,922,976,544,921,700,000,000 |
| attacktype1_txt | 15 | 133,844,648,173,825,000,000,000 |
| weaptype1_txt | 15 | 2,007,669,722,607,380,000,000,000 |
| hostkidoutcome_txt | 17 | 34,130,385,284,325,500,000,000,000 |
| claimmode_txt | 18 | 614,346,935,117,859,000,000,000,000 |
| weapsubtype4_txt | 20 | 12,286,938,702,357,200,000,000,000,000 |
| gsubname2 | 24 | 294,886,528,856,572,000,000,000,000,000 |
| region_txt | 26 | 7,667,049,750,270,880,000,000,000,000,000 |
| dbsource | 26 | 199,343,293,507,043,000,000,000,000,000,000 |
| weapsubtype3_txt | 30 | 5,980,298,805,211,280,000,000,000,000,000,000 |
| targtype3_txt | 34 | 203,330,159,377,184,000,000,000,000,000,000,000 |
| targtype1_txt | 37 | 7,523,215,896,955,790,000,000,000,000,000,000,000 |
| targtype2_txt | 37 | 278,358,988,187,364,000,000,000,000,000,000,000,000 |
| gname3 | 43 | 11,969,436,492,056,700,000,000,000,000,000,000,000,000 |
| targsubtype3_txt | 88 | 1,053,310,411,300,990,000,000,000,000,000,000,000,000,000 |
| natlty3_txt | 93 | 97,957,868,250,991,800,000,000,000,000,000,000,000,000,000 |
| divert | 138 | 13,518,185,818,636,900,000,000,000,000,000,000,000,000,000,000 |
| country_txt | 213 | 2,879,373,579,369,650,000,000,000,000,000,000,000,000,000,000,000 |
| natlty1_txt | 216 | 621,944,693,143,845,000,000,000,000,000,000,000,000,000,000,000,000 |
| kidhijcountry | 219 | 136,205,887,798,502,000,000,000,000,000,000,000,000,000,000,000,000,000 |
| gname2 | 223 | 30,373,912,979,066,000,000,000,000,000,000,000,000,000,000,000,000,000,000 |
| gsubname | 728 | 22,112,208,648,760,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 |
| gname | 3182 | 70,361,047,920,354,400,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 |

# Strategic Economic Decision-Making (Grover, 2013)

- In this manuscript, I evaluated ten likely scenarios:

1. Manufacturing Risk
2. Political Risk
3. Gambling Risk
4. College Entrance Exams & Freshman retention Risks
5. Currency Market Risks
6. Acts of Terrorism Risks
7. Default Risks
8. Insurance Risks
9. Special Forces Assessment and Selection Risks (Level I)
10. Special Forces Assessment and Selection Risks (Level II)

# Lessons Learned

- Post publication of SEDM

—**Agriculture community** I learned by trying to operationalize BBN in conducting R&D in the Agriculture community in determine which 500 varieties out of hundred of thousands were ones that needed to be selected in the maturation process of selecting the most promising ones that would have the greatest yield in the next phase of selection.

--**Special operations recruiting** I learned working with the US Army Recruiting Command that there are similarities to the agriculture R&D work that organizations are looking for decisions based on needle in the haystack selection outcomes. Selecting niche Soldiers with characteristics based on success in the past is uniquely Bayes'.

--**Medical Recruiting** I learned had the same characteristics as the Agriculture and Special Operations Recruiting—niche market requirements of small numbers out of a large population.

# Global Terrorism

- Given these number of row outputs in a dataset such as the **Global Terrorism database**, it becomes very clean using manual methods of calculating these posterior probabilities is not feasible. Human calculation error alone begins at the 3 and 4 event levels.

  - It has taken a week to **manually calculate six events** with small number of ME elements per event.

- A BBN algorithm easily slices through some of these paths. **Traditional statistical methods** such as deductive hypothesis testing simply cannot match the capabilities of BBN.

# BBN Utility

- A **server-side BBN algorithm** can be used to analyze data in a wide range of industries. Examples include

  **--Agriculture** Identifying crop yield based on climate, soil quality, genetics, etc.

  **--Finance** Classifying bankruptcy risks of companies based on size, revenues, etc.

  **--Military** Identifying Soldiers with the greatest likelihood of becoming Special Forces

  **--Retail** Choosing prices for a good or service to maximize profits

  **--Human Resources** Identifying the ideal candidate for a particular position

  **--Marketing** Targeting consumers, i.e. via social media data

- This list continues to grow as more organizations in increasingly diverse fields begin to collect information and store it in big datasets. The applications of the **BayeSniffer algorithm** are only limited by the availability of data.

# Conclusions

- This presentation presented an overview of the need for a **server-based algorithm**, provided a background of its theoretical foundations, gave a detailed example of its application to terrorism research, and listed a number of other possible applications.

- The **BayeSniffer algorithm** is a unique and proprietary data-sniffing tool built based on the concept of the SEDM that translates data into actionable intelligence through a client-server approach.

  --Once data are uploaded, we sniff through them, extract useful results using inductive logic (Plato), and present clear interpretations. In a market flooded with data-mining protocols, we establish our niche in evaluating data using conditional probabilities and Bayesian statistics.

# Strategic Economic Decision-Making Conclusions

- In **strategic decision-making**, it is very clear that at each level of a management decision chain, for example a government bureaucracy, each decision-maker has not only decisions that effect their level, but they are motivated to include information from each subordinate level.

--This is a leveraging effect, like illustrated here again. If we consider each level of a bureaucracy as events in the terrorism example, then if a supervision is at Level 6, then there could at a minimum be 2 x 2 x 2 x 2 x 2 x 2 = 64 paths to evaluate.

| Event | # ME-E | # Paths (Rows) |
|---|---|---|
| extended | 2 | 2 |
| crit1 | 2 | 4 |
| crit2 | 2 | 8 |
| crit3 | 2 | 16 |
| gsubname3 | 2 | 32 |
| guncertain1 | 2 | 64 |
| vicinity | 3 | 192 |
| doubtterr | 3 | 576 |
| multiple | 3 | 1,728 |
| success | 3 | 5,184 |
| suicide | 3 | 15,552 |
| guncertain2 | 3 | 46,656 |
| guncertain3 | 3 | 139,968 |
| INT_LOG | 3 | 419,904 |
| INT_IDEO | 3 | 1,259,712 |
| INT_MISC | 3 | 3,779,136 |
| INT_ANY | 3 | 11,337,408 |
| alternative | 4 | 45,349,632 |
| alternative_txt | 4 | 181,398,528 |
| claim3 | 4 | 725,594,112 |
| compclaim | 4 | 2,902,376,448 |
| ishostkid | 4 | 11,609,505,792 |
| ransom | 4 | 46,438,023,168 |
| claimed | 5 | 232,190,115,840 |
| specificity | 6 | 1,393,140,695,040 |
| property | 6 | 8,358,844,170,240 |
| propextent | 6 | 50,153,065,021,440 |
| weaptype4_txt | 8 | 401,224,520,171,520 |

- We are **challenged at every level** to include not only the information available to our current decision-making level but to those **below** and **above** us.
- Now, given current computer technology and the constructs of **Bayes’ theorem using BBN**, this is feasible.

# References


- Global Terrorism Website, Global Terrorism database. (**National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2013). Global Terrorism Database [Data file]. Retrieved from http://www.start.umd.edu/gtd).**
- Grover, J (2013). Strategic Economic Decision-Making. (http://www.springer.com/statistics/book/978-1-4614-6039-8).
- Grover, J (2014). White Paper: Strategic Economic Decision-Making: Using Bayesian Belief Networks to Make Complex Decisions. MORS Symposium. Washington, DC.
- Rankins, R, Bertucci, P, Gallelli, C, & Silverstein, A (2013). *Microsoft SQL Server 2012*. SAMS publishing, Pearson Education.
- Stanford Encyclopedia of Philosophy. Plato Inductive Logic. (Retrieved from http://plato.stanford.edu/entries/logic-inductive/#3.3).
- The BayeSniffer Server-Side Algorithm, BayeSniffer.com.